

January 28, 2002

From: Shakeel Mustafa
24831 Hendon Street
Laguna Hills, CA 92653
Tel:- 949-457-1243

To: US Patent and Trademark Office
Washington DC. 20231
Fax: 703-746-7239

Re: Petition for making the Patent Application 09/848,670, as a Special Case on the basis of its disclosure of sensitive and strategic information in the interest of National Security.

Dear Sir/Madam,

I have filed a patent application 09/848,670, Filing date 05/04/2001 with your office. The invention titles "System and Method for encrypting and decrypting information through the use of random numbers". The invention discloses an innovative and robust encrypting/decrypting technology that can be used to transmit/receive any type of digital information in a secure manner.

Therefore, it is requested that said patent application should be considered as a special case on the basis that it discloses information, which can be strategically important to National Security. In addition to the submitted patent application for your review please also enclosed find Annex A to be read in conjunction with the said patent application that explains the patent's versatility and robustness.

Please feel free to write or call me if you have any questions. I look forward to receiving your feedback on this matter.

Sincerely,

Shakeel Mustafa



UNITED STATES PATENT AND TRADEMARK OFFICE

COMMISSIONER FOR PATENTS
UNITED STATES PATENT AND TRADEMARK OFFICE
WASHINGTON, D.C. 20231
WWW.USPTO.GOV

APPLICATION NUMBER	FILING DATE	GRP ART UNIT	FIL FEE REC'D	ATTY. DOCKET NO	DRAWINGS	TOT CLAIMS	IND CLAIMS
09/848,670	05/04/2001	2131	373	SH0004	14	22	3

CONFIRMATION NO. 7787

FILING RECEIPT



OC000000006236072

SHAKEEL MUSTAFA
15520 TUSTIN VILLAGE WAY Apt. # 2
TUSTIN, CA 92780

Date Mailed: 06/28/2001

Receipt is acknowledged of this nonprovisional Patent Application. It will be considered in its order and you will be notified as to the results of the examination. Be sure to provide the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION when inquiring about this application. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. If an error is noted on this Filing Receipt, please write to the Office of Initial Patent Examination's Customer Service Center. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections (if appropriate).

Applicant(s)

Shakeel Mustafa, Tustin, CA;

Domestic Priority data as claimed by applicant

Foreign Applications

If Required, Foreign Filing License Granted 06/27/2001

Projected Publication Date: 11/07/2002

Non-Publication Request: No

Early Publication Request: No

** SMALL ENTITY **

Title

System and method for encrypting and decrypting information through the use of random numbers

Preliminary Class

380

Annex A

Robustness of the Encryption/Decryption Technology disclosed in the Patent Application 09/848,670

The following section illustrates the robustness, simplicity and versatility of the patent pending technology. As disclosed in the patent application the encryption strength of the said technology depends upon the different number of combinations and permutations that can be produced through using the techniques presented in this invention. In a typical situation the following parameters can be used.

Size of the seed random number = 128 bits

Number of bits assigned as Group Bits = 4 bits

Number of bits assigned as Function Bits = 6 bits

Total number of mathematical and/or logical Functions defined = 64 Functions

Average number of Functions performed on an information block = 16 functions.

The total number of possible combinations using the 4 Group Bits in a 128 bits number can be given as

$$(128)^4 = 268.43 \times 10^6 \text{ combinations}$$

The total number of possible combinations using the 6 Functions Bits in a 128 bits number can be given as

$$(128)^6 = 4.398 \times 10^{12} \text{ combinations}$$

The total number of all possible combinations for Group and Function Bits (10 bits) together in a 128 bits number can be found as

$$(128)^{10} = 1.180 \times 10^{21} \text{ combinations}$$

The total number of all possible functions that 16 functions randomly selected from the function pool consisted of 64 functions can be given as

$$(64)^{16} = 7.922 \times 10^{28} \text{ possible number of functions performed.}$$

The above presented scheme presents such a powerful encryption method that an eavesdropper who may even have complete access and knowledge of all the functions defined in the first and the second pool on both the remote and at the host will not be able to decrypt an encrypted information block. For example, if a would-be code breaker can execute about 200 billions functions per second in order to decrypt an information block, it would take him 39.42×10^{15} seconds or 12.5 billions years to process all the possible number of functions, i.e., 7.922×10^{28}

A continuous change and update between a host and remote about the designated location of Group and Function Bits assigned within a random number will make the unauthorized decryption task impossible and prohibitive.
